DES JOUETS INQUIÉTANTS

Les jouets connectés qui inquiètent plus qu'ils n'amusent. Equipés de connexions Bluetooth et Wi-Fi, ces robots et peluches interagissent avec les enfants. A chacun sa vocation. L'ours en peluche Teddy Toy-Fi transmet les messages vocaux enregistrés par leurs parents depuis leur smartphone, via une application dédiée. Le robot i-Que raconte des blagues, propose des quizz et des jeux interactifs. Le dinosaure Cognitoys répond aux questions et fait travailler le vocabulaire... Tous se connectent à Internet pour puiser les réponses aux questions et les messages stockés sur des serveurs distants. Seulement voilà, certains jouets connectés sont de vraies passoires. Trois des sept testés n'exigent ni mot de passe, ni code PIN pour une connexion Bluetooth. N'importe qui peut donc s'y connecter très facilement, même à travers les murs. Un voisin mal intentionné pourrait envoyer un message au robot iQue et écouter les réponses de l'enfant. « *Cette faille de sécurité est extrêmement critique, explique Stiftung Warentest. Toute personne qui possède un smartphone peut contrôler le robot, l'utiliser comme mouchard, adresser des questions, des invitations, voire des menaces à l'enfant* ». De même, n'importe qui peut envoyer des messages à l'ourson Toy-Fi. Quant au chien connecté Wowwee Chip, un tiers pourrait également en prendre le contrôle et diriger ses mouvements (mais pas communiquer avec l'enfant).

DES DONNEES DANS LA NATURE...

Stiftung Warentest a par ailleurs constaté des problèmes de sécurisation des transmissions de données. Quatre des jouets testés sont concernés. Plus précisément, ce sont les applications qui servent à piloter ces jouets qui posent problème. Ces applis, disponibles sur l'App Store et le Google Playstore, collectent des données sur les utilisateurs (e-mail, âge des enfants, etc.) et sur les smartphones (identification, opérateur mobile). Certaines enregistrent également les paroles des enfants, des fichiers audio stockés ensuite sur des serveurs. Hello Barbie, la poupée connectée de Mattel, les met même à disposition des parents sur Internet (des fois qu'ils tiennent à écouter leurs enfants à distance). Heureusement, aucune des applications testées n'envoie de données sans cryptage. Mais aucune n'exige non plus de mot de passe complexe (comprenant des caractères minuscules, majuscules, des caractères spéciaux, des chiffres). Dès lors, les découvrir est un jeu d'enfant pour des pirates un brin expérimentés. Nos collègues allemands ont aussi constaté, sur différentes applications, l'envoi d'informations à Google ou à des tiers à des fins publicitaires, et le recours à des traceurs capables, a priori, de reconstituer les déplacements des parents.

...ET DU PIRATAGE DANS L'AIR

Ces négligences révèlent l'insouciance des fabricants de jouets connectés qui pourrait, au final, coûter cher aux parents. Certaines applications proposent du contenu payant et sont donc susceptibles de stocker leur numéro de carte de paiement. « *Si les serveurs du fabricant sont mal sécurisés, des pirates peuvent accéder facilement aux comptes utilisateurs et pourquoi pas faire des achats sur le compte des parents* », alerte Stiftung Warentest. Preuve que les jouets connectés intéressent les pirates : Spiral Toys, qui commercialise les peluches Cloudpets, en a déjà été la cible au début de l'année. Fin 2016, la poupée Mon amie Cayla avait été mise en cause : n'importe qui pouvait parler à travers la poupée et écouter les personnes autour d'elle via une simple connexion Bluetooth de son smartphone. En 2015, les serveurs de l'entreprise VTech avaient déjà été piratés. Ces problèmes de sécurité informatique sont inquiétants. C'est pourquoi, fin 2016, l'UFC-Que Choisir a saisi la CNIL (Commission nationale de l'informatique et des libertés) et la DGCCRF (Direction générale de la concurrence, de la consommation et de la répression des fraudes) afin qu'elles enquêtent sur la protection des données personnelles des utilisateurs de jouets connectés.